LA-UR-01-6817

Approved for public release;
distribution is unlimited.

Title: PRESENT AND FUTURE FREE-SPACE QUANTUM KEY DISTRIBUTION

Author(s):
JANE E. NORDHOLT, P-21, M/S D454, 7-3897
RICHARD J. HUGHES, P-23, M/S H803, 7-3876
GEORGE L. MORGAN, P-23, M/S H803, 7-1137
CHARLES G. PETERSON, P-23, M/S H803, 5-1368
CHRISTOPHER C. WIPF, P-23, M/S H803

Submitted to:
SPIE CONFERENCE:
FREE-SPACE LASER COMMUNICATIONS TECHNOLOGIES XIV
20-25 JAN 2002
SAN JOSE, CA

Present and Future Free-Space Quantum Key Distribution

Jane E. Nordholt[*a], Richard J. Hughes[**b], George L. Morgan[b], Charles G. Peterson[b], Christopher C. Wipf[b]

[a]Biophysics Group, Los Alamos National Laboratory
[b]Neutron Science and TechnologyGroup, Los Alamos National Laboratory

ABSTRACT

Free-space quantum key distribution (QKD), more popularly know as quantum cryptography, uses single-photon free-space optical communications to distribute the secret keys required for secure communications. At Los Alamos National Laboratory we have demonstrated a fully automated system that is capable of operations at any time of day over a horizontal range of several kilometers. This has proven the technology is capable of operation from a spacecraft to the ground, opening up the possibility of QKD between any group of users anywhere on Earth. This system, the prototyping of a new system for use on a spacecraft, and the techniques required for world -wide quantum key distribution will be described. The operational parameters and performance of a system designed to operate between low earth orbit (LEO) and the ground will also be discussed.

Keywords: quantum cryptography, quantum key distribution, free-space, optical communications

1. INTRODUCTION

The information age has ushered in a tremendous need for secure high-speed information transfer. Information transfers are typically secured by the use of cryptographic systems which require relatively short (typically a few hundred bits) random bit sequences called cryptographic keys. These systems may be either symmetric or asymmetric. In asymmetric systems, keys can be widely distributed and used to send messages to the owner of the key. These keys can however only be used to send messages one-way and they are dependent on the assumed difficulty of certain mathematical calculations such as factoring large numbers. These techniques have not been proven to be uncrackable and could all be useless in short order if a new algorithm is invented that speeds up the mathematical calculations that they use. Symmetric systems require that both users have a copy of the same key. Delivery of these keys generates huge logistics problems. Each user who wishes to communicate must have a set of random numbers delivered before the communications session can begin. Today, symmetric keys are often delivered by asymmetric cryptography systems which may make them equally vulnerable. Symmetric keys delivered by couriers may seem to be a more secure system because their security does not depend on unproven mathematical assumptions, but the difficulties of frequent deliveries lead to many potentially more severe security threats. The random numbers thus delivered must be generated and prepared in advance for delivery and then stored in secure locations until needed. This provides a would-be spy with opportunities to copy keys when they are being delivered or stored.

Once the users of symmetric systems have keys in hand from whatever delivery technique, they must have an agreed upon way of using them to encrypt and decrypt their messages. The best-known example of this type of cryptography is the onetime pad. In the case of a onetime pad, the key must be as long as the message to be sent. The sender, typically called Alice, converts the message she would like to send into numbers then XORs each bit from the message with a bit from the random numbers of the onetime pad. The message Alice then sends looks to the rest of the world like random numbers. The recipient, typically referred to as Bob, has a copy of the same onetime pad and XORs each bit of it with the bits he received from Alice. Now Bob can read the message. This system is unconditionally secure if the key material is properly safeguarded. However for large amounts of data, delivery of so much random key material is

[*] JNordholt@LANL.gov; phone 1 505 667-3897; fax 1 505 665 5507; Los Alamos National Laboratory, M/S D454, Los Alamos, NM 87545; [**]Hughes@LANL.gov; phone 1 505 667-3876; fax 1 505 665-4121; Los Alamos National Laboratory, M/S H803, Los Alamos, NM 87545

prohibitive. Many systems rely on random number generators to produce the large number of random bits needed. These systems need a key large enough that an adversary who is forced to search all possible keys is confounded. Quantum cryptography has been developed to securely deliver these valuable random key strings on demand and as such is more properly called quantum key distribution (QKD). The quantum mechanical properties of single photons can be exploited to provide secure key distribution. Figure 1 shows the basic ideas behind quantum key distribution. Alice and Bob have both a quantum channel and a conventional channel for communications between them. The quantum channel is simply a medium such as an optical fiber or a free space path that allows single quanta to be transmitted faithfully. The conventional channel can be anything from an Ethernet connection, to a telephone line, to an optical communications link. There are several QKD protocols and quantum mechanical properties which can be used to transmit information on the quantum channel but for free space quantum key distribution we have chosen to use a protocol known as BB84 (for Bennett and Brassard 1984)[1,2], and the polarization of single photons as our quantum mechanical information bearing quantity.

There are five steps to generating a secret key with quantum cryptography: authentication; single photon transmissions; sifting; error correction; and privacy amplification. Authentication must be performed so that Alice knows that she is in fact communicating with Bob. If Alice and Bob cannot authenticate contact, a clever eavesdropper, commonly referred to as Eve, would be able to convince Alice that she is Bob and Bob that she is Alice. This is called a man-in-the-middle attack and without authentication cannot be prevented. Authentication is often performed by Alice and Bob using some bits from their previous secret key to check each other's identities. In free space QKD authentication can possibly be achieved by Alice and Bob imaging each other. This may require a very sophisticated adaptive optical system but without it Alice and Bob still have to rely on couriers for their initial start-up authentication bits.

Once Alice and Bob are convinced that they are communicating with each other, Alice starts the protocol by generating pairs of random bits. The first bit of each pair determines in which basis Alice will transmit the value of the second random bit. A basis is a set of two orthogonal polarization states that have been defined to represent either a 0 or 1. Alice uses a pair of bases which are not orthogonal to each other (they are should be offset by 45˚) so that a photon measured with a polarizer set for the wrong basis returns a random result. Alice then proceeds to send Bob a string of non-orthogonally polarized photons. Ideally each bit is sent with exactly one photon, however true single photon sources are rare. We use highly attenuated laser pulses which will occasionally send more than 1 photon. Alice does not reveal what the correct basis for each photon was until it has been received and measured. This is the quantum part in quantum cryptography and what the rest of this paper will focus on. It is essential however, if security is to be maintained, that the rest of the steps involved in generating a key be performed correctly. These steps also determine the final secret key bit yield and are a major factor in the realization of a practical QKD system.

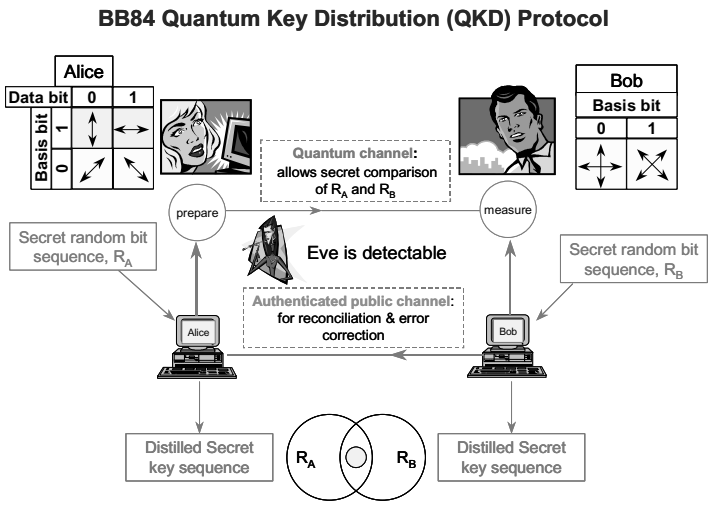

Figure 1. Overview of BB84 and QKD.

In each of Alice's polarization bases she has orthogonal polarizations defined to be either 0 or 1. The two bases are however, 45º apart. This means that if the basis in which Alice sends a photon is known, the photon can be accurately measured to determine its bit value. However Alice uses random bases, which are unknown to both Bob and to any eavesdroppers who try to intercept them. Without knowledge of the basis used, Bob randomly selects a basis in which to measure Alice's photons. He then measures each photon to decide whether it was a 0 or 1 and records both the basis in which he measured and the value he determined. If Bob measured in the wrong basis, his polarization analysis system was at 45º to the actual polarization of the incoming photon and his measured bit value is completely random. He next contacts Alice on the conventional channel and tells her which photons

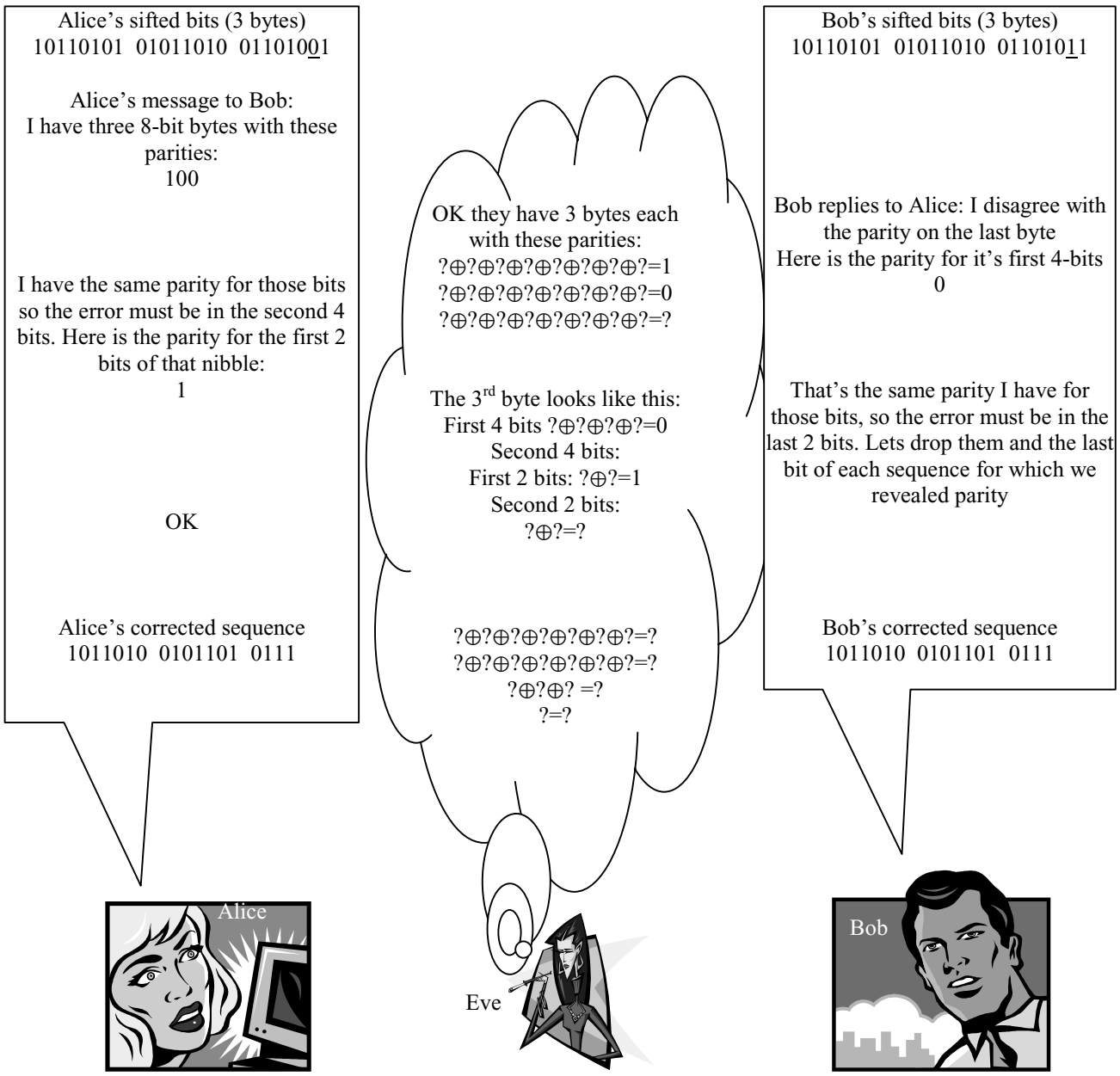

Figure 2. In this example Alice and Bob have a single error in their sifted bit sequence (underlined character in their starting sequences). They use multiple parity checks to find and remove the error. At this point Eve has some knowledge of their sequence from listening to this public discussion, but Alice and Bob sacrifice some of their bits so that their final sequence is completely unknown to Eve.

he measured and in which basis. Alice replies, telling Bob which bits he measured in the correct basis and should therefore keep. The other bit values are discarded. Although this sacrifices half of the bits Alice sent to Bob, it provides protection from eavesdropping for the remaining bits. This process is called sifting and in a perfect system Alice and Bob would now have a common secret random bit sequence. At no point do Alice and Bob reveal whether the photons received were ones or zeros. So an eavesdropper listening in on the conventional channel would not have gained any

information about the bit sequences Alice and Bob now have. An eavesdropper on the quantum channel would have to be bold enough to undertake an active attack instead of just passive eavesdropping because single photons cannot be split. Any photon Eve measures is altered and cannot be split or copied and sent on to Bob. This makes it possible for Alice and Bob to monitor an eavesdropper's activities on the quantum channel because an eavesdropper will cause errors (differences) in Alice and Bob's sifted keys. Alice and Bob then use techniques from information theory to reduce Eve's knowledge of their key sequences to less than 1 bit of information. This will be discussed in more detail below.

Alice and Bob now have sifted sequences of random bits which would complete the protocol if detectors and single photon sources were perfect and background could be completely eliminated so that there were no errors. In the real world, there will be errors and Alice and Bob must next find a way to correct these errors. Of course, it is impossible for Alice and Bob to find errors in their shared secret sequences without revealing something about their sequences to Eve. Alice and Bob can encode their discussion using some key material they already have or they can keep careful track of what information they reveal and use techniques such as that shown in Figure 2 to later remove from their shared sequences any information Eve might have gained from Alice and Bob's error correction discussion on the public channel. In either case Alice and Bob have to sacrifice some key bits to find the errors in their sequences. Alice and Bob then have a shorter string and a good estimate of the number of the errors they had in their sifted sequences, the bit error rate (BER). In practice because parity checks can only find an odd number of errors in a bit sequence, sifted bits are shuffled and then checked for errors several times. All errors must be eliminated to a high degree of certainty. If Alice and Bob's keys differ by even a single bit they will be unusable.

Because Alice and Bob are only trying to build up a shared secret random sequence of numbers and they begin with random sequences, any photons that don't reach Bob do not affect the security of the final key. If an eavesdropper intercepts a photon it can be lost without affecting the security of the system. A more clever eavesdropper who tries to measure the photon and send it on to Bob will not know what basis to use and because the bases are non-orthogonal, when Eve selects the wrong basis, which will be 50 percent of the time, she will have a 50 percent chance of measuring a 45º photon as either 0 or 1. When she tries to send this on to Bob she will introduce a 50% error rate in those bits. As described below, Alice and Bob monitor their bit error rate (BER), so that they can put a rigorous upper bound on the amount of information Eve might have about their shared sequences. They can then correct for any information an eavesdropper might have discovered.

In the final step, Alice and Bob use the error rate information from the previous step and knowledge of the quantum mechanical and physical principles of the technique and system operation to put a rigorous upper bound on the possible information that Eve may have about their bit sequences. They assume that the BER was entirely caused by Eve's attempts to measure single photons and further that Eve has intercepted and measured a photon from every multi-photon pulse. These are very rigorous assumptions but necessary if security is to be guaranteed. Alice and Bob then apply a technique called "privacy amplification"[3,4] to reduce Eve's maximum possible knowledge about their shared secret strings to less than 1 bit. Alice and Bob XOR together sequences of bits (e.g. $1 \oplus 1 = 0$; $1 \oplus 0 = 1$) to produce new bits. The amount of compression required depends on the estimate of Eve's knowledge. If the original sequence is n-bits in length it is compressed with privacy amplification to R(n) bits where $R(n) = - n \log_2 [\varepsilon^2 + (1-\varepsilon)^2]$, n is the original number of bits and ε is Eve's BER. As an example, if Alice and Bob know that Eve knows 3 out of 6 bits they can apply privacy amplification to eliminate that knowledge. If Alice and Bob's shared sequence is 6-bits, a,b,c,d,e,f, they can make 2 new bits out of the original 6 by XOR-ing them as follows:

$$a \oplus b \oplus c \oplus d = \text{bit } 1$$
$$c \oplus d \oplus e \oplus f = \text{bit } 2$$

If only 1 bit in a sequence in unknown then the parity (XOR of all the bits) is unknown. Since Eve knows at most 3 bits of the entire sequence she knows nothing about the new bits generated by this procedure. Alice and Bob estimate Eve's knowledge/bit (50% means that Eve can only guess the correct value), and therefore her entropy/bit, and privacy amplification decreases Eve's knowledge/bit and increases her entropy. Because Alice and Bob have a way of putting an upper bound on Eve's knowledge of their shared sequence, Alice and Bob can apply privacy amplification to reduce Eve's knowledge to less than 1 bit in a key several hundred bits in length. Alice and Bob have then produced an information-theoretically secure key.

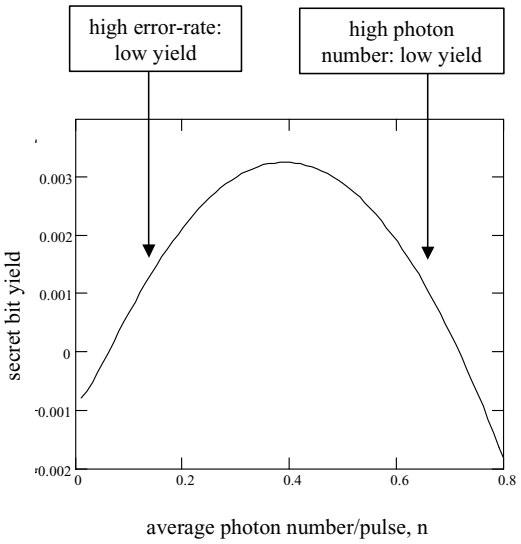

Figure 3. Secret bit yield vs. $\overline{n}$ the average number of photons sent per pulse.

One last consideration is to prepare for the next key generation session by saving some secret bits for authentication.

The secret bits required to carry out both the error correction and privacy amplification schemes in QKD reduce the number of secret bits generated by the single photon transfers. In the real world, this loss of key bits is unavoidable because the errors that occur from background light or dark counts in detectors must be attributed to the actions of an eavesdropper. If the BER is too high or link rates are too low, there will be insufficient sifted key bits from the quantum channel to perform the full protocol. It is therefore essential to do experiments to test out all aspects of the protocol under realistic conditions where the calculated error rates can be verified and the hardware and software can be optimized.

Free-space QKD experiments have demonstrated that the optimal number of photons for Alice to send Bob is dependent on the atmospheric conditions between the two. If Alice chooses a very low average photon number such as 0.1 photons per pulse, most of the time she sends nothing and link efficiency on the quantum channel will be very poor. If Alice chooses a high average photon number per pulse, an eavesdropper can in principle split out and identify one of the photons of every multi-photon pulse. Figure 3 shows a typical curve of average photon number vs. secret bit yield when all of the error correction and privacy amplification needed to make a secure system have been taken into account. A true single photon source would increase the secret bit yield of our system.

2. CURRENT INSTRUMENTATION

One of the most demanding aspects of QKD is the need to pick single photons out from the background of daylight photons which is often of the order of 10^{12} / cm^2-s-Å-ster. Figure 4 shows typical plots of the daytime atmospheric transmission and background power for a range of wavelengths for which optics and detectors can be obtained. It may be noted that background is generally decreasing with increasing wavelength while the transmission is increasing. This makes it appear that operation at longer wavelengths might be attractive. However single photon detectors that operate at longer wavelengths than those shown in Figure 4 (e.g. InGaAs avalanche photodiodes), have very high background rates and low efficiencies relative to those available in the shorter wavelengths. Fieldable, high-efficiency single photon detectors are essential for the quantum communications channel. There are two commercially available candidate

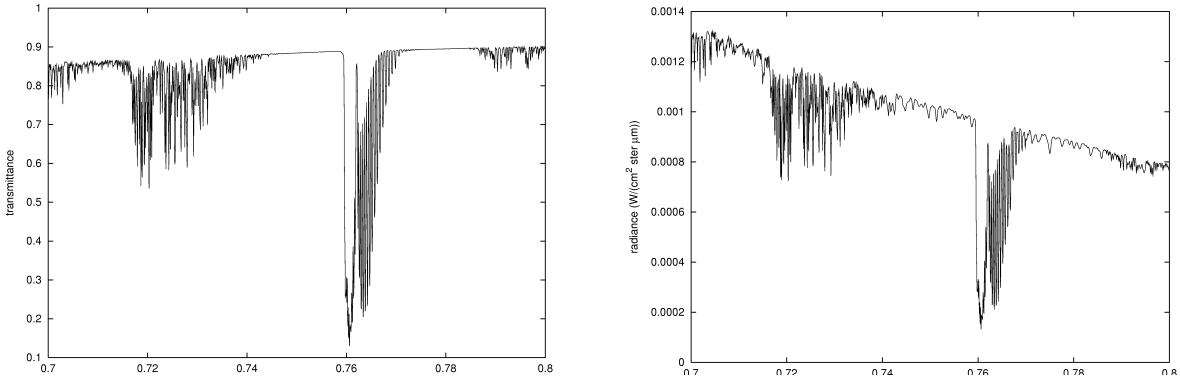

Figure 4. Transmission and radiance of the atmosphere at relevant wavelengths

methods for efficiently detecting single photons: Si avalanche photo diodes (APDs) and photomultiplier tubes (including hybrid photo detectors which have similar quantum efficiency curves). When typical atmospheric background and transmission are convolved with the coupling and detection efficiencies of a complete system, expected secret bit yields can be calculated using the response curve for each type of detector. Figure 5 shows the expected bit yields under the same atmospheric conditions for systems employing the two types of detectors. The increased operational wavelengths of Si APDs and their higher quantum efficiency give systems employing them secret bit yields approximately an order of magnitude higher than those employing PMTs. The maximum of the secret bit yield curve occurs at ~776 nm. The availability of suitable laser diodes and the preferred operating temperature have dictated operation at 772 nm in our current system. This provides a secret bit yield very near the optimal operation point. Our system also includes a bright timing pulse that carries no polarization information and can be as bright as needed to ensure detection. It is also beneficial if the wavelength of the bright pulse is outside the sensitivity window of the single photon detectors. We have chosen 1550 nm for this wavelength because of its relative eye-safety at the required power of a few mW.

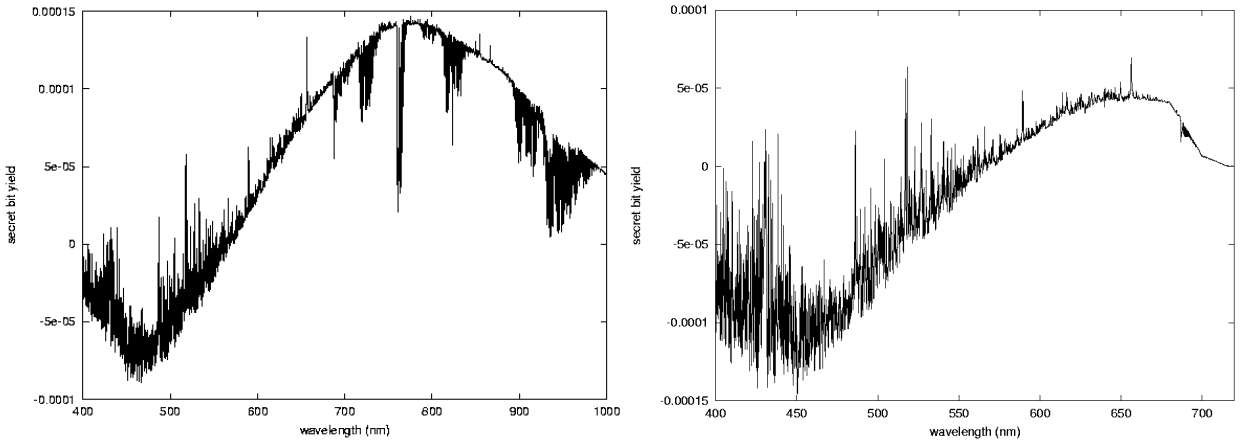

Figure 5. The secret bit yields vs. relevant wavelengths for common atmospheric and daylight background conditions over the same path to space from Los Alamos, NM for systems using Si APDs(left-hand panel) and PMTs/hybrid photo detectors (right-hand panel).

To reliably detect the single photons sent by Alice, Bob and Alice employ several "tricks." Spatial, spectral, and temporal filtering are needed. Spatial filtering requires a narrow acceptance angle and accurate pointing of the receiver. We use a 220-microradian acceptance angle and require that level of stability and tracking accuracy in Bob's receiving optics. This gives eight orders of magnitude reduction in background over the acceptance of a bare detector. Alice and Bob also use narrow wavelength filters. Our wavelength filters are 1 Å full width at half maximum and provide several orders of magnitude reduction in background over what would be experienced by a bare detector. Filtering in the time domain requires another trick. Alice sends a bright pulse a few nanoseconds before she sends a single photon pulse. Bob easily detects the bright signal, which allows him to gate his detectors so that he accepts only photons that occur in that narrow time window. The atmosphere can cause changes in the photon's time of flight but these variations occur over a time span of ~10ms so the few ns between the bright pulse and data pulse is consistently maintained. If a 1 ns time window is used with a repetition rate of 1 MHz, time filtering in this way gives three orders of magnitude reduction in background. We find an acceptable daylight background rate of ~40 kHz with about 1 kHz of dark noise in the SPCMs. The BER in our system is typically on the order of a few percent.

Figure 6 shows the QKD transmitter and receiver, Alice and Bob, as they currently exist at Los Alamos National Laboratory (LANL). They are mounted in transportable trailers for easy setup at distant locations and have been used for both long distance demonstrations and short distance tuning and analysis runs. Polarization states are generated by Alice by triggering of one of four 772 nm data lasers, each of which has its own attenuator, focusing optics, and polarizers to produce a pulse of the desired brightness in one of the four required polarization states. The four lasers

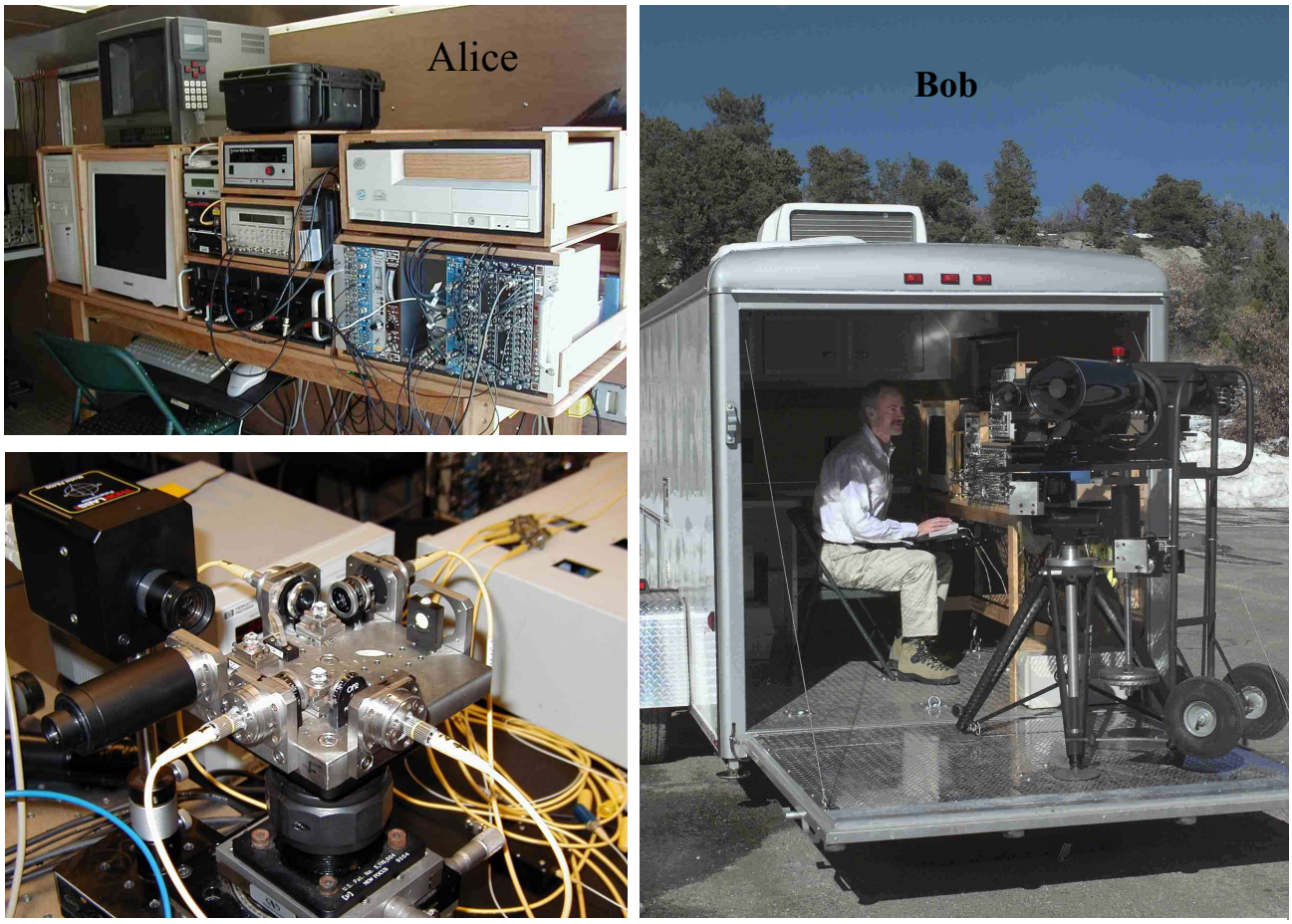

Figure 6. The LANL Free-Space QKD system. Alice's electronics and the optical bench which holds fiber launch and beam combining optics to produce the 4 polarization states is on the left. Bob's electronics and optics are visible in their mobile trailer on the right.

represent each of the two bases' two data states (0 or 1). The output of all four data lasers is combined by a series of beam splitters which have been carefully arranged so that all of the distances between the data lasers and output optics are the same. Because the bright pulse sets up a timing window for the data pulses, if any data laser was placed farther from the output path than the others, it might be possible to detect that bit value without producing any increase in BER. The output of the beam splitters is then sent into a single mode fiber which serves as a final mode filter before output to the transmit optics. In this way no mode information, which might inadvertently reveal which laser fired, is transmitted. The 1 Å filter also serves to eliminate any wavelength information that might reveal information about the data laser that fired.

To send a bit Alice first sends a bright pulse at 1550 nm, she then fires a 772 nm laser with the desired polarization. To maximize coupling efficiency Alice must be precisely pointed at Bob. Bob analyzes Alice's single photon by first randomly selecting a polarization basis with a beam splitter. He then rotates the polarization of the incoming photon so that a polarizing beam splitter can send the photon to the "0" or "1" detector in that basis. Four Si APD, single-photon counting modules (SPCMs), one at each of the output ports of the two polarizing beam splitters (one in each basis), determine where the photon emerges and thus its polarization data state. If however, the randomly selected basis is not the same as the one used by Alice the result will be random and those bits will not be part of the sifted key.

The free-space QKD system at LANL has proven to be operable under a wide range of atmospheric and daylight conditions including light snow and rain, and very close proximity of the transmitter to the direction of the Sun.

3. FUTURE FREE-SPACE QKD

The results obtained to date with the current LANL free-space QKD system have given us the data needed to determine the technique's applicability in practical situations. Near-ground paths of several km are achievable and make it possible to provide secure communications on optical data lengths in cities and across and between corporate or government campuses.[5,6] It should also be possible to re-key satellites on orbit with QKD.[7] Satellites are extremely valuable assets requiring secure command, control, and data paths in order to protect their operations and capabilities. QKD to spacecraft awaits the launch of a purpose-built QKD transmitter or receiver. However the data from the current system can be used in a preliminary design study of the feasibility of QKD to spacecraft.

The operation of a QKD system to space does not require that both the transmitter, Alice, and the receiver, Bob, be designed to withstand space flight environmental conditions. QKD requires only a one-way transmission of photons so Alice and Bob need not both go into space. Both the transmitter and receiver have some requirements that require careful consideration if they are to be used in space. A spacecraft can provide only limit power, temperature control, volume, and mass allowances so the flight module must be capable of realization inside these limitations. Both the transmitter and receiver shown in Figure 6 can be miniaturized for space flight, but there are further considerations based on the required optical and electronic components for each module.

Alice requires a smaller optical aperture than Bob but more accurate pointing. She also requires temperature-controlled lasers and interference filters to maintain the needed narrow wavelength passband. The lasers must be temperature controlled otherwise their output would drift in and out of the passband causing variation in the average number of photons in the transmitted pulses. Likewise the interference filters must be temperature controlled to prevent their wavelength from drifting. Another advantage of sending Alice into space is that her optical system can couple to the transmitting system on the spacecraft by mean of a short piece of single-mode optical fiber. This gives a designer more freedom in the placement and orientation of the transmitter module than the receiver module which must have a direct line-of-sight to the receiving optics.

Bob has a less accurate pointing requirement than Alice but requires a larger aperture, a disadvantage on a spacecraft that can also limit the allowable pointing accuracy. Accurate pointing to a spacecraft through atmospheric turbulence is easier from a well-stabilized ground-based platform but variations in the atmosphere make it difficult to track a beacon from a spacecraft and accurately send photons back to the spacecraft. The motion of the spacecraft means that it will be in a different patch of atmosphere, outside the isoplanatic angle as seen from the ground, by the time beacon photons are received and QKD photons can be transmitted. Bob also contains SPCMs that would have increased noise from the penetrating radiation in space. These detectors and Bob's wavelength filter also need to be temperature controlled.

Both the transmitter and receiver modules have precise optical alignment and timing requirements and will need additional temperature control to maintain them in space. The system as a whole will require a high-speed telemetry link so that Alice and Bob can perform the communications required to complete the QKD protocol. Also required is the ability of one module to track the polarization orientation variation of the spacecraft as it passes overhead. A polarization "zero" direction can be defined by a beacon from either Alice or Bob and corrected by rotation of a half-wave plate at whichever module is on the ground. The polarization tracking will be performed by the ground-based component to save weight and complexity on the

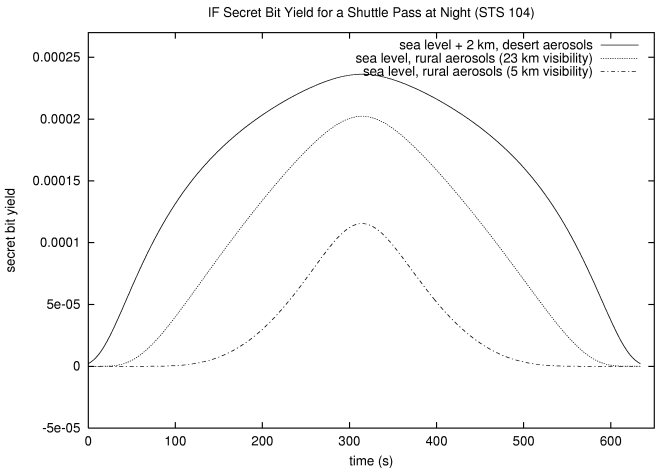

Figure 7. Secret bit yield to low Earth orbit at night. Yield is secret bit number/s divided by photon pulses transmitted/s.

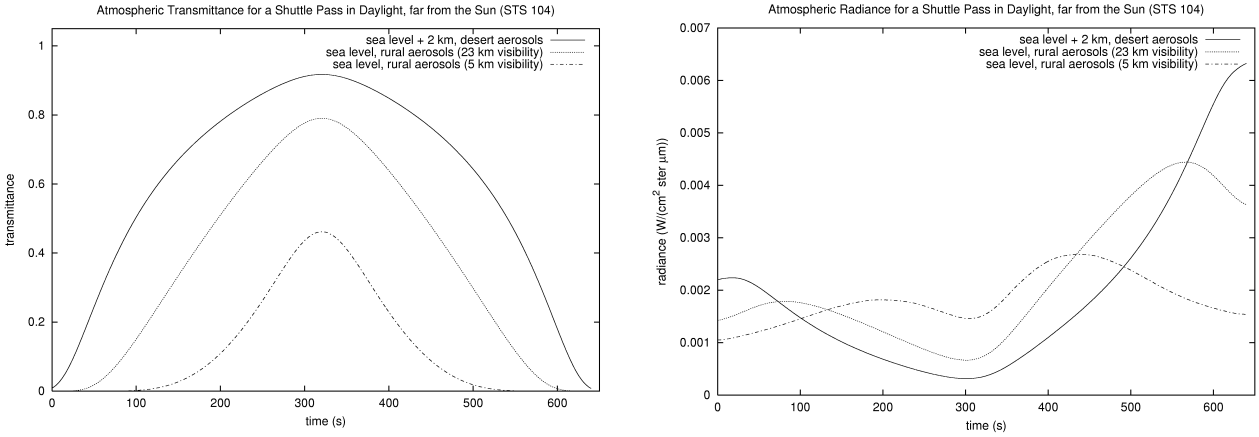

Figure 8. Atmospheric transmittance and radiance for a typical shuttle pass where the Sun is not near the field of view.

space-based component.

For these reasons, preliminary designs for QKD to spacecraft are based on a system design where the transmitter is flown. The receiver remains on Earth and carries out the polarization-tracking task. Some spacecraft may not have the stability needed to make it possible for the transmitter to accurately point at a receiver but this system is not intended for use on all possible spacecraft.

Calculations of the QKD bit yield for a system with the transmitter in a low Earth orbit (LEO) have been carried out using a system design similar to the current one with some small modifications. A 50 cm aperture has been assumed for the receiver along with 5μrad pointing. The transmitter is 10 cm in diameter and able to accurately point at a beacon from the receiver. A 1 Å wavelength filter and a 39 μrad field-of-view are assumed. The spacecraft is assumed to be in a 700 km LEO orbit similar to that of a typical space shuttle mission or the international space station. At this distance through atmospheric turbulence, a 10 cm transmitter aperture and a 50 cm receiver have a calculated beam coupling efficiency of approximately a 1%. Figure 7 shows the expected secret bit yield for this system during a relatively high (up to 70˚ in elevation) nighttime pass of the satellite overhead. Nighttime background is sufficiently low that the changes in the secret bit yield are entirely due to the varying optical depth of the atmosphere as the satellite moves through different elevation angles. Even ground station sites with relatively poor visibility and low altitudes are able to perform QKD with positive bit yields for hundreds of seconds. With an expected transmission rate of 10 MHz the expected secret bit yield can be over 1 kHz for at least part of the pass even in relatively poor atmospheric conditions.

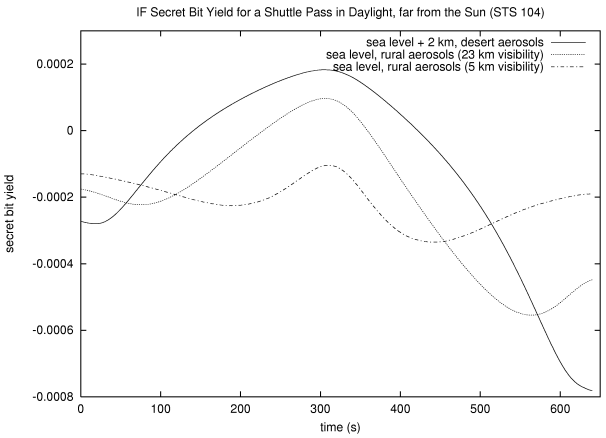

Figure 9. Secret bit yield to the low Earth orbit shuttle/ISS daylight pass shown in Figure 8.

For daylight QKD sessions, the angle of the Sun to the spacecraft's track and the Sun's elevation angle are all important in determining the background light level and the error rate it produces in the QKD system. Figure 8 shows atmospheric transmission and radiance along the track of a shuttle pass where the Sun is low in the sky (15˚ elevation) but never closer to the spacecraft track than 65˚ in azimuth. The atmospheric transmission is again a function of the track elevation (a maximum of 60˚) but the background illumination varies considerably with the relative position of the Sun.

Figure 9 shows the secret bit yield expected. Note that for this pass the expected BER is high enough that QKD for some portions of the pass would produce a negative yield which is to say that, if the QKD protocol were carried out during these portions of the orbital pass, more key bits would be used than produced. The importance of a site with good visibility is clear.

Figure 10 shows the secret bit yield for a satellite pass that reaches an elevation of only 40º and passes within about 20º of the Sun's position. In this case only a high clear desert site has a possibility of producing any secret bits. If a narrower wavelength filter is used, positive bit yield can be obtained for all but the lowest visibility site. However the narrower wavelength filter (0.01 Å was assumed) would require real-time adjustment of the center wavelength of the filter's passband to correct for the Doppler shift caused by the spacecraft's motion.

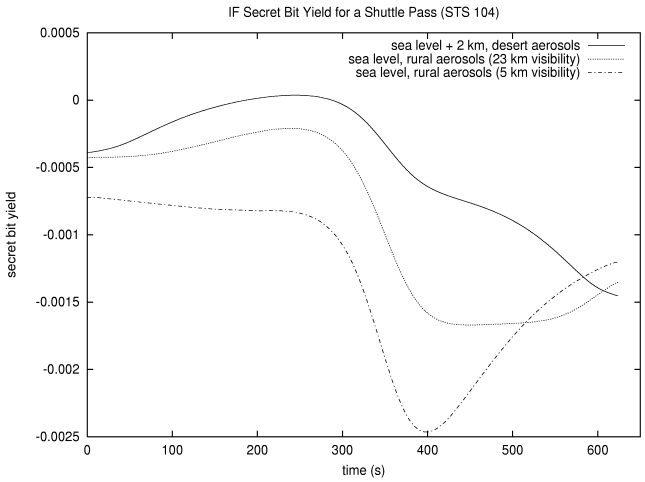

Figure 10. Secret bit yields for a shuttle pass within 10˚ apparent angle from the sun.

QKD is possible between satellites and a wide range of ground station locations, satellite passes, and atmospheric conditions. This wide range of possible satellite contacts opens up other applications for QKD. To date free-space QKD has been limited to users who have a line-of-sight path between them, however, employing free-space QKD to satellites offers the possibility of securely re-keying cryptographic systems for users anywhere on Earth. Each user separately generates a key with a trusted satellite. The satellite then tells users which bits they should change in order to have the same key as the first user. Because each key generation session has been carried out securely, and the additional information which needs to be transmitted is only which bits a user should change, not any bit values, these shared keys would be as secure as those generated directly by the users. In this way, free-space QKD promises to make on-demand keys available to users anywhere a trusted satellite or group of satellites can be seen.

4. SUMMARY

Free-space QKD is a new development that promises long-term security for high-value data. Our system has demonstrated that with careful selection of the operational wavelengths, system components, and mathematical algorithms it uses, it can be made sufficiently robust to be deployed anywhere in the world. QKD to satellites in low Earth orbit should also be possible under a wide variety of conditions. Re-keying satellites with QKD not only would provide their command and control systems a very high level of security, it would also make it possible to distribute cryptographic keys to users anywhere on Earth.

ACKNOWLEDGEMENTS

The authors would like to thank D. Derkacs for technical support.

REFERENCES

1. C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984,* (IEEE, New York, 1984), P. 175, 1984.

2. G. Brassard and C. H. Bennett, "Quantum Cryptography," *Lecture Notes In Computer Science* , **325**, pp. 79-90, 1988.

3. C. H. Bennett *et al*., “Privacy amplification by public discussion,” *SIAM Journal on Computing*, **17**, no.2, pp. 210-229, April 1988.

4. C. H. Bennett, *et al*., “Generalized privacy amplification,” *IEEE Trans. Inform. Theory* **41**, no. 6, part 2, pp. 1915-1923, 1995

5. R. J. Hughes *et al.*, “Daylight quantum key distribution over 1.6 km,” *Physical Review Letters*, **84**, pp. 5652-5655, 2000.

6. R. J. Hughes *et al.,* “Free-space quantum key distribution in daylight,” *Journal of Modern Optics*, **47**, 549, 2000.

7. R. J. Hughes *et al.*, "Quantum cryptography for secure satellite communications," *IEEE Aerospace 2000 Conference*, Big Sky, Montana, March 14-25, 2000.